De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets

Oerlemans, J.J.; Koops, E.J.

Published in:
Nederlands Juristenblad

Publication date:
2011

Document Version
Peer reviewed version

De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets
Jan-Jaap Oerlemans en Bert-Jaap Koops[1]

[gepubliceerd in *86 Nederlands Juristenblad* (18), p. 1181-85]

Op 28 november 2010 begon WikiLeaks met de publicatie van 251.287 diplomatieke stukken van Amerikaanse ambassades en consulaten. In reactie hier op weigerden hostingaanbieder Amazon en financiële dienstaanbieders MasterCard, Visa, PayPal en BankFinance nog langer hun diensten te verlenen aan de klokkenluidersorganisatie. Een 'hacktivisten'-groep genaamd Anonymous viel de bedrijven vervolgens aan met zogenoemde distributed Denial-of-Service-aanvallen (verstikkingsaanvallen), waardoor bepaalde websites onbereikbaar waren en sommige diensten niet meer geleverd konden worden.[2] De vraag is hoe ernstig dergelijke aanvallen zijn: gaat het om een digitale protestactie of een ernstig misdrijf, en zo ja, welk misdrijf dan precies? In zijn arrest van 22 februari 2011 maakt de Hoge Raad duidelijk dat in Nederland financiële diensten als 'vitale infrastructuur' kunnen worden gerekend. [3] Degene die deze diensten aanvalt riskeert een maximale gevangenisstraf van 6 jaar. Dat is zelfs wanneer - zoals bij de online betalingsdienst PayPal – de betalingsdienst nog gewoon functioneert.

De Hoge Raad geeft in het arrest echter een onlogische en volgens ons onwenselijke uitleg aan de wet door het begrip 'gemeen gevaar voor verlening van diensten' (art. 161sexies Sr) erg op te rekken. Bovendien stelt de Hoge Raad in hetzelfde arrest ten onrechte het plaatsen van malware gelijk aan computervredebreuk. Deze extensieve interpretaties komen de rechtszekerheid niet ten goede. In deze bijdrage wordt het onderhavige arrest nader bestudeerd en uiteengezet waarom de magistratuur met het arrest de samenleving een slechte dienst heeft bewezen.

De feiten
Tussen 1 juni 2005 tot en met 4 oktober 2005 heeft de verdachte in deze zaak een virus verspreid, dat bekend is geworden onder de naam 'Toxbot'. Het virus kon zich over andere nog niet geïnfecteerde computers verspreiden en was daarmee technisch gezien een worm, maar we zullen Toxbot in het vervolg aanduiden onder de meer gebruikelijke aanduiding virus. Op 8 augustus 2010 waren 50.095 computers besmet. Deze computers vormden samen een botnet, dat wil zeggen een netwerk van besmette computers die op afstand via een *command-and-control*-server door een derde kunnen worden aangestuurd. Het Toxbot-virus had bovendien een 'keylogger-functionaliteit', waarmee toetsaanslagen konden worden opgenomen en heimelijk doorgestuurd. De functionaliteit wordt in het bijzonder gebruikt voor het afvangen van gebruikersnamen en wachtwoorden. Met deze

[1] Mr. Jan-Jaap Oerlemans is promovendus bij eLaw@Leiden, centrum voor recht in de informatiemaatschappij, Universiteit Leiden. Daarnaast is hij juridisch adviseur bij Fox-IT. Prof.dr. Bert-Jaap Koops is hoogleraar regulering van technologie bij TILT – Tilburg Institute for Law, Technology, and Society, Universiteit van Tilburg.
[2] C. Bryan-Low en S. Grundberg, 'Hackers Rise for WikiLeaks, *Wall Street Journal* 8 december 2010 http://online.wsj.com/article/SB10001424052748703493504576007182352309942.html (laatst geraadpleegd op 7 april 2011).
[3] HR 22 februari 2011, *LJN*: BN9287. In navolging van Rb. Breda, 30 januari 2007, *LJN*: AZ7281, Rb. Breda, 30 januari 2007, *LJN*: AZ7266 en Hof 's-Hertogenbosch, 12 september 2008, *LJN*: BF0770.

gegevens kan een hacker gebruik maken van diensten van het slachtoffer en bij gegevens komen die normaal gesproken zijn afgeschermd.

De besmette computers konden tevens de opdracht krijgen een bepaald Trojaans paard (genaamd 'Wayphisher') te downloaden en te installeren op de computer van het slachtoffer. Een Trojaans paard is een onschuldig lijkend programma met kwaadaardige functionaliteiten. Na besmetting van de computer met Wayphisher wordt de computergebruiker omgeleid naar een andere website. Deze phishingwebsite lijkt op een normale webpagina van een bank waarbij bezoekers worden aangespoord hun gegevens in te vullen, zoals rekeningnummers en wachtwoorden die nodig zijn voor de aangeboden dienst. Deze gevoelige gegevens worden door Wayphisher afgevangen en doorgestuurd naar de command-and-control-server waar de gegevens vervolgens door de dader kunnen worden opgehaald en worden misbruikt voor frauduleuze transacties. In de Toxbot-zaak werd duidelijk dat een groot aantal computers besmet zijn geraakt met Wayphisher.

Het Openbaar Ministerie heeft de verdachte twee delicten ten laste gelegd, namelijk (1) een gekwalificeerde vorm van computervredebreuk zoals bedoeld in artikel 138a lid 3 Sr (oud) en (2) computersabotage als bedoeld in artikel 161sexies lid 1 aanhef en onderdeel 2 Sr. Het eerste is ten laste gelegd, omdat de verdachte met het virus is binnengedrongen in de besmette computers en zich vervolgens via de command-and-control server (impliciet) toegang heeft verschaft tot de computers van derden. Wat het tweede delict betreft zou artikel 161sexies Sr van toepassing zijn. Computergebruikers die besmet waren met het Toxbot-virus en het Trojaanse paard Wayphisher, werden namelijk doorgeleid naar een phishing-website en konden daardoor niet op behoorlijke wijze gebruik maken van (financiële) diensten van algemene nutte. Daarnaast zou ook het onderscheppen van financiële gegevens en wachtwoorden een gemeen gevaar voor dienstverlening hebben opgeleverd.

Het Hof had verdachte voor het eerste feit – computervredebreuk – veroordeeld, maar vrijgesproken van computersabotage omdat niet de computer van een nutsdienst maar alleen computers van eindgebruikers waren geïnfecteerd, zodat er geen gemeen gevaar voor dienstverlening ontstond. De Hoge Raad laat de veroordeling voor het eerste in stand maar casseert de vrijspraak op het tweede punt: volgens hem is er ook bij stoornis in computers van gebruikers sprake van gemeen gevaar voor dienstverlening.

Bij beide punten willen wij in deze bijdrage vraagtekens plaatsen. Volgens ons wordt te makkelijk aangenomen dat het verspreiden van een virus computervredebreuk oplevert, en wordt de reikwijdte van 161sexies Sr onnodig ver opgerekt.

Computervredebreuk

In het arrest staat ter discussie of er bij het Toxbot-virus wel een beveiliging is doorbroken (wat tot 2006 een eis voorwaarde was voor toepasselijkheid van 138a-oud Sr), omdat het virus gebruik maakte van een lacune in de beveiliging van Windows XP. Het systeem was volgens de verdediging daarmee niet beveiligd. Zowel Hof als Hoge Raad maken korte metten met deze redenering: het is niet relevant of een hacker gebruik maakt van een opening die inherent is aan het systeem of die is veroorzaakt door een aanvaller,

zolang er maar sprake is van ‘enige beveiliging’ op de computer. Deze conclusie is terecht.

Waar onze kritiek zich op richt betreft een ander punt, waartegen de verdediging (naar we aannemen) geen verweer heeft gevoerd. Het Hof en de Hoge Raad gaan ervan uit dat door de infectie met het Toxbot-virus wordt binnengedrongen in een computer. ’s Hofs bewezenverklaring luidt hier dat verdachte en medeverdachte ‘de toegang hebben verworven door een technische ingreep (...), namelijk telkens door, gebruikmakend van één of meer kwetsbaarheden in het besturingssysteem van Windows, een (al dan niet door verdachte gemaakte/ontwikkelde) versie van een virus, onder meer bekend onder de naam Toxbot, te (doen) verspreiden en/of te (doen) installeren’. Met andere woorden: het (doen) verspreiden of (doen) installeren van een virus levert hacken (computervredebreuk) op. Deze lezing van het Hof en de Hoge Raad is opmerkelijk, omdat de wetgever bij de Wet computercriminaliteit[4] bewust verschillende strafbaarstellingen heeft ingevoerd voor hacken (138a-oud) en voor virusverspreiding (art. 350a lid 3 Sr). De Hoge Raad laat deze twee nu feitelijk samenvallen, met als enige verschil dat voor virusverspreiding niet nodig is dat het virus ook daadwerkelijk een computer binnendringt – het enkele versturen is voldoende. Virusverspreiding is dan simpelweg een strafbare voorbereidingshandeling voor hacken.[5] In deze interpretatie kan de strafbaarstelling van virussen wel worden afgeschaft, omdat er altijd sprake zal zijn van een strafbare poging tot hacken. Zodra het virus wordt losgelaten, hangt het immers van omstandigheden buiten de wil van de verdachte af of het virus erin slaagt een computer te infecteren (en daarmee te hacken).

Volgens ons kan niet simpelweg gesteld worden dat het enkele infecteren van een computer met een virus ook computervredebreuk oplevert. De strafbaarstelling van hacken is vormgegeven naar analogie met huisvredebreuk (art. 138 Sr): het wederrechtelijk binnendringen in een computer respectievelijk woning. Bij binnendringen denkt men aan een persoon die zich begeeft in een ruimte. Eventueel kan men dat oprekken tot een deel van de persoon, zoals in het ‘arm-arrest’ waarbij alleen de arm in de woning komt,[6] en wellicht zelfs tot het binnendringen met een verlengstuk van de persoon (zoals een wandelstok die de grens van de woning overschrijdt). Maar je kunt moeilijk zeggen dat er wordt binnengedrongen in een ruimte wanneer iemand niet in directe verbinding staat met die ruimte. Dat is echter wat het geval is bij een computervirus: de dader stuurt een virus ongericht de wereld in en heeft vervolgens niet als zodanig[7] een verbinding met de computers die worden geïnfecteerd.

---

[4] *Stb*. 1993, 33.

[5] Merk op dat de wetgever bij de Wet computercriminaliteit II, *Stb*. 2006, 299, art. 350a lid 3 Sr een voorbereidingshandeling heeft genoemd, maar niet van hacken; het gaat om ‘een *voorbereidingshandeling*: strafbaar is degene die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die bedoeld zijn ‘*om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk*’, aldus *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 36 (onze cursivering).

[6] HR 7 februari 1956, *NJ* 1956, 147.

[7] Bij een botnet kan er wel sprake van een verbinding; daarop gaan we hieronder in.

Toegegeven: veel vormen van malware[8] staan tegenwoordig in verbinding met de verspreider ervan. Dit gaat door middel van een botnet, waarbij de dader via een command-and-control-server de geïnfecteerde computers kan aansturen door er commando's aan toe te zenden. Deze commando's worden in een rechtstreekse verbinding door de dader verzonden aan de zombiecomputers, die veelal ook gegevens (zoals onderschepte wachtwoorden) terugzenden aan de command-and-control-server. In dat geval kun je volgens ons wel, volgens een 'verlengde arm'-constructie, spreken van computervredebreuk. Maar het is dan wel belangrijk om onderscheid te maken in de stadia waarin een botnet tot stand komt: het binnendringen in de zin van art. 138ab Sr vindt pas plaats op het moment dat daadwerkelijk gebruik wordt gemaakt van de functionaliteit van een botnet. Bij het opzetten van een botnet, door het versturen van een virus zoals Toxbot en het afwachten tot geïnfecteerde computers zich 'melden' bij de command-and-control-server, is er nog geen sprake van binnendringen – hooguit van een (mogelijk strafbare) poging daartoe.

Het Openbaar Ministerie zou dus scherper moeten zijn bij een tenlastelegging met betrekking tot een botnet en duidelijker uit elkaar houden welke handelingen als het verspreiden van een virus (350a lid 3 Sr) en welke handelingen als het binnendringen in een computer (art. 138ab Sr) kunnen worden gekwalificeerd. Wat de strafmaat betreft hoeft het OM niet bang te zijn om het verspreiden van Toxbot-achtig virus als virusverspreiding ten laste te leggen: op overtreding van art. 350a lid 3 Sr staat dezelfde maximumstraf van vier jaren als bij gekwalificeerd hacken (art. 138ab lid 3 Sr) en een geldboete van een hogere categorie.

Computersabotage

Ten tweede is de interpretatie van de Hoge Raad met betrekking tot artikel 161sexies Sr interessant. Dit artikel stelt strafbaar het verstoren van een computer of telecommunicatiewerk waardoor gemeen gevaar of levensgevaar ontstaat. Een website van een bank, een online betalingsdienst als PayPal, een veilingdienst als Ebay en creditcardmaatschappijen kunnen een 'dienst van algemene nutte' aanbieden. Dergelijke diensten hebben veelal een publieke functie in het economisch verkeer en bij het onbruikbaar maken van een dergelijke dienst kan dan ook artikel 161sexies Sr van toepassing zijn.[9] Wel zijn wij van mening dat onderscheid moet worden gemaakt in wat er precies wordt verstoord, bijvoorbeeld welk onderdeel van de website wordt aangevallen. Immers, indien door een DDoS-aanval (een verstikkingsaanval die een website uit de lucht haalt) een informatiepagina van een online betalingsdienst wordt aangevallen heeft dat andere gevolgen dan wanneer de pagina's niet meer bereikbaar zijn die nodig zijn voor het transactiesysteem. Onzes inziens is artikel 161sexies Sr alleen van toepassing wanneer een website van een dienst ten algemene nutte wordt aangevallen waardoor gevaar ontstaat dat de dienst zelf niet meer kan worden verleend.

[8] De term 'malware' is een samentrekking van 'malicious' en 'software', oftwel kwaadaardige software. Het is een verzamelterm voor virussen, wormen en Trojaanse paarden.

[9] Vgl. de conclusie van Knigge bij HR 22 februari 2011, *LJN*: BN9287: "Bedoeld lijkt te zijn dat de toenemende afhankelijkheid van de samenleving van die geautomatiseerde opslag en verwerking maakt dat daarmee algemene belangen zijn gemoeid en dat daarom strafbaarstelling als gemeengevaarlijk delict gerechtvaardigd is" (par. 26).

Belangrijker is echter de extensieve interpretatie die de Hoge Raad aan artikel 161sexies Sr geeft. Zij stelt namelijk dat ook het ontnemen van de mogelijkheid van een substantieel aantal *afnemers* van diensten van algemene nutte artikel 161sexies lid 1 onderdeel 2 Sr kan constitueren. Voor de duidelijkheid: het gaat hier niet meer om de computer van een nutsdienst zelf, maar om de computers van (een substantieel aantal) afnemers die gebruik maken van diensten van algemene nutte.
De Hoge Raad redeneert als volgt. Tekstueel gezien wordt bij de term 'geautomatiseerd werk' geen onderscheid gemaakt tussen computers van dienstverlenende instellingen en computers van afnemers van diensten. Ook in de wetgeschiedenis wordt dat onderscheid niet gemaakt. Onder het bestanddeel 'gemeen gevaar' in artikel 161sexies Sr moet daarom worden verstaan: *"het gevaar voor een ongestoorde dienstverlening aan een onbestemd doch aanmerkelijk aantal afnemers"*.[10] Volgens de Hoge Raad gaat het uiteindelijk om de vraag of de opzettelijk veroorzaakte stoornis een gemeen gevaar voor een ongestoorde dienstverlening teweeg brengt. In de Toxbot-zaak konden de slachtoffers van het computervirus niet meer op een veilige wijze gebruik maken van de diensten van bancaire instellingen of creditkaartmaatschappijen, aangezien hun computers besmet waren met malware. Artikel 161sexies lid 1 onderdeel 2 Sr is om die reden van toepassing.

Op dit punt wijkt de Hoge Raad af van de conclusie van Advocaat-Generaal Knigge. Knigge beargumenteert dat artikel 161sexies Sr ziet op het de geautomatiseerde werken van de dienstaanbieder zelf. Het vernielen van een groot aantal computers van dienstafnemers levert, elk afzonderlijk, geen gevaar op voor de dienstverlening van de dienstaanbieder. 'Als een bende onverlaten plunderend door de stad trekt en met knuppels alle personal computers die zij aantreft, in elkaar slaat, is het effect daarvan dat een grote groep burgers internetbankieren wel even kan vergeten. Maar dat wil niet zeggen dat de groep onverlaten zich schuldig heeft gemaakt aan het medeplegen van art. 161sexies Sr'.[11] Wij onderschrijven de conclusie van Knigge dat artikel 161sexies Sr ziet op het vernielen van een specifieke computer dat tot gevolg heeft dat dienstverlening van algemene nutte gevaar loopt, en niet op de cumulatie van afzonderlijke computers die eventueel van een dienst van algemene nutte gebruik maken. De tekst van het artikel geeft daarvoor een duidelijke aanwijzing: 'Hij die opzettelijk *enig* geautomatiseerd werk (…) vernielt [enz.] wordt gestraft (…) 2°. met gevangenisstraf (…) indien *daarvan* gemeen gevaar voor goederen of voor de verlening van diensten te duchten is (…)' (onze cursivering). Het moet dus gaan om gemeen gevaar dat wordt veroorzaakt door het vernielen van enige computer; de tekst suggereert geenszins dat het gevaar ook zou kunnen ontstaan door een optelsom van vernielingen terwijl elke afzonderlijke vernieling als zodanig geen gevaar oplevert.

De interpretatie die de Hoge Raad geeft aan artikel 161sexies Sr impliceert echter dat ook de vernieling van een substantieel aantal computers die door klanten voor internetbankieren worden gebruikt, het gemeengevaarlijke delict van artikel 161sexies Sr

[10] HR 22 februari 2011, *LJN*: BN9287, r.o. 3.5.
[11] HR 22 februari 2011, *LJN*: BN9287, par. 20 (concl. A-G Knigge).

oplevert.[12] Maar zoals A-G Knigge ook nog opmerkt, wordt in artikel 161sexies gesproken over de *verlening* van een dienst van algemene nutte en niet het *gebruik* ervan. In combinatie met de formulering 'enig geautomatiseerd werk (…) indien daarvan gemeen gevaar (…) te duchten is' kan het artikel dan ook bezwaarlijk anders worden gelezen dan als een strafbaarstelling van sabotage van de computer van de *aanbieder* van een dienst ten algemene nutte.
Terecht stelt Knigge dat als artikel 161sexies Sr niet van toepassing is, het gedrag zeker niet straffeloos is; artikel 350a lid 3 Sr kan nog steeds van toepassing zijn. Wij kunnen daar nog diverse andere bepalingen aan toevoegen die evenzeer van toepassing lijken op het feitencomplex: gegevensaantasting (art. 350a lid 1 Sr), phishing (wat oplichting oplevert, art. 326 Sr), misbruik van hulpmiddelen (art. 139d lid 2 Sr) en, door de keylogging-functionaliteit van Toxbot, aftappen (artikel 139c Sr en 139d lid 1 Sr).

Kortom, wij zijn van mening dat de redenering van Advocaat-Generaal Knigge meer hout snijdt dan die van de Hoge Raad. Artikel 161sexies Sr beschermt tegen de nadelige effecten die optreden indien de infrastructuur van de dienstverlener wordt vernield of beschadigd, en dient niet ter bescherming van de vertrouwelijkheid en integriteit van de computer van de dienstafnemer(s). De interpretatie van de Hoge Raad rekt de reikwijdte van het artikel op, waardoor art. 161sexies nauwelijks nog onderscheidende waarde heeft. Met de redenering van de Hoge Raad gaat 161sexies immers elke verspreiding omvatten van malware die een substantieel aantal computers aantast, waardoor gebruikers niet goed meer kunnen internetbankieren, skypen, internet-tv kijken of op de webpagina van hun energieleverancier kunnen kijken. Dat heeft niets meer te maken met een gemeengevaarlijk delict, maar alles met 'gewone' computercriminaliteit die in de diverse andere bepalingen in het wetboek is strafbaar gesteld.

Conclusie
Terecht hecht de Hoge Raad waarde aan de afhankelijkheid van onze samenleving van ICT. Het online betalingsverkeer is in de loop der jaren een onmisbare dienst geworden van Nederlandse burgers. Het kan gerechtvaardigd zijn dat het verstoren van grote aantallen computers waarbij de gebruikers niet langer normaal kunnen internetbankieren, zwaar wordt gestraft. Het is echter niet nodig om daarvoor art. 161sexies Sr van stal te halen. Het is moeilijk te achterhalen waarom precies het OM dit artikel ten laste heeft gelegd in plaats van het meer voor de hand liggende art. 350a lid 3 Sr (virusverspreiding) of art. 139c Sr (aftappen). Ook had het OM zich kunnen baseren op andere artikelen, zoals het opzettelijk en ongevraagd toevoegen van software (art. 350a lid 1 Sr) of het plaatsen van een keylogger (art. 139d lid 1 Sr).[13]
Het is ook speculeren waarom de Hoge Raad, anders dan het Hof, het OM volgt met een gekunstelde argumentatie die de reikwijdte van 161sexies erg oprekt. Wellicht speelt hier parten dat in het verleden 161sexies wel is gebruikt om cyberaanvallen te vervolgen, zowel op overheidswebsites[14] als op webpagina's van e-handelaars[15]. Destijds was dat

[12] Vgl. HR 22 februari 2011, *LJN*: BN9287, par. 27 (concl. A-G Knigge).
[13] Merk op dat inmiddels ook nog twee andere bepalingen toepasbaar zijn op een feitencomplex als in de Toxbotzaak: oplichting door phishing (art. 326 Sr) of het verspreiden van een hulpmiddel voor hacken (art. 139d lid 2 Sr). Deze waren ten tijde van de Toxbotfeiten (in 2005) nog niet in werking.
[14] Rb. 's-Gravenhage 14 maart 2005, *LJN*: AT0249.

nodig omdat er geen specifieke strafbepaling bestond voor dit type aanvallen. Die lacune is in 2006 gedicht met art. 138b Sr. Sindsdien is er geen reden om art. 161sexies Sr als een vangnet te zien voor veelomvattende cyberaanvallen.

Evenzo is het onnodig en onwenselijk om bij verspreiding van Toxbot-achtige virussen direct uit te gaan van computervredebreuk. Hoewel de functionaliteit van dit type virussen – waarbij een aanvaller via een command-and-control-server commando's geeft aan geïnfecteerde computers – impliceert dat computers kunnen worden gehackt, betekent het verspreiden van en computers infecteren met van zo'n virus als zodanig nog geen computervredebreuk. Dat is pas het geval als de dader daadwerkelijk met de geïnfecteerde computers communiceert.

De Nederlandse strafwetgeving kent een genuanceerd scala aan bepalingen die elk verschillende typen van cyberaanvallen omvatten. Het is belangrijk dat OM en de rechterlijke macht precies zijn in de toepassing van de verschillende delicten op een feitencomplex zoals in de Toxbot-zaak. Door de extensieve interpretatie die nu wordt gegeven aan zowel art. 138ab als art. 161sexies Sr verwatert het onderscheid tussen de verschillende typen computerdelicten. Dat doet geen recht aan de inspanningen van de wetgever om een dekkend systeem van computercriminaliteitsbepalingen tot stand te brengen. Bovendien is het slecht voor de rechtszekerheid, omdat kwestieuze (en extensieve) interpretaties door toekomstige rechters kunnen worden omzeild of teruggedraaid, waardoor vervolgingen kunnen stuklopen. Al met al bewijst het optreden van de magistratuur in de Toxbot-zaak daarom de systematiek van de computercriminaliteitswetgeving een slechte dienst.

[15] Hof 's-Hertogenbosch 12 februari 2007, *LJN*: BA1891; in deze zaak werd vrijgesproken omdat een aanval op de webpagina van een enkel e-handelbedrijf geen gemeen gevaar voor dienstverlening oplevert.